

ASSISTANCE FROM THE NORTH AMERICAN SECURITIES ADMINISTRATORS  
ASSOCIATION FOR STATE-REGISTERED INVESTMENT ADVISERS SEEKING TO  
COMPLY WITH THE PRIVACY DISCLOSURE PROVISIONS OF THE GRAMM-LEACH-  
BLILEY ACT

On November 12, 1999, President Clinton signed into law the Gramm-Leach-Bliley Act (GLBA).<sup>1</sup> GLBA eliminated legal barriers between the securities, insurance, and banking industries, but retains the oversight roles of federal and state agencies within their particular areas of expertise.

One of the major components of GLBA is the creation of new privacy laws and regulations.<sup>2</sup> The new privacy requirements went into effect on November 13, 2000, and compliance will be mandatory on July 1, 2001.<sup>3</sup>

This document is being provided to you and other investment advisers to assist you in complying with the new privacy laws. It is designed to make you aware of the new regulatory requirements and to help you think through potential civil liabilities for failure to develop and implement privacy policies and practices. It is not legal advice. You may want to consult an attorney regarding the applicability of GLBA's privacy provisions to you.

**Summary of GLBA**

GLBA's new privacy laws regulate what you are allowed to do with the confidential personal information that you collect in connection with your investment advisory activities. Specifically, these provisions govern how you collect, use, and maintain this personal information and under what circumstances you may share it with someone else. The law requires that you adopt written policies for handling confidential personal information and that you properly distribute those written policies.

In general, GLBA prohibits you from sharing an individual's confidential information with non-affiliated third parties, unless:

- You tell the individual that you may share the information with others;
- You give the individual the opportunity to tell you not to share the information; and
- The individual does not tell you to keep the information confidential (i.e., the individual does not "opt out" of disclosure to third parties).<sup>4</sup>

The following is a more in-depth discussion of the new regulatory requirements.

**Definitions**

Some definitions are in order, so that you can decide which people, and what information you obtained from or about those people, are included in the concept of confidential personal information.

GLBA distinguishes between a customer and a consumer. A customer<sup>5</sup> is a person with whom you have developed a continuing relationship to provide products or services to be used for primarily personal, family, or household purposes. A customer would *not* include a person who met with someone from your firm, but then decided not to establish a business relationship with your firm. So we can distinguish the difference between the two types, we will call the latter person a consumer.<sup>6</sup>

Non-public personal information (“NPI”)<sup>7</sup> is any personal information that cannot be found in public sources. Publicly available information would be details available from federal, state, or local government records; widely distributed media (such as telephone directories or newspapers); or information disclosed to the public as required by federal, state, or local law. NPI is usually obtained directly from the individual. It includes such details as the person’s date of birth, social security number, financial account numbers and balances, sources and amounts of income, credit card numbers, information obtained about visitors to your Internet web site, and sometimes could include home addresses and telephone numbers.

An affiliate<sup>8</sup> is a company that controls, is controlled by, or is under common control with your firm. A non-affiliated third party<sup>9</sup> is any person or entity other than your firm, your employee, or an affiliate.

Opt-out<sup>10</sup> is a concept requiring you to give consumers and customers notice that NPI may be disclosed to third parties. It includes giving them the chance to “opt out” of such disclosure and telling them how to exercise that right.

A joint marketer<sup>11</sup> is a person or company who markets your products or services under a joint agreement with one or more financial institutions. A service provider<sup>12</sup> is a person or company who assists your firm in administering, processing, or servicing a customer’s account.

### **Notice Requirements**

Under GLBA, each investment adviser must give its *customers* either a full notice or simplified notice of the firm’s privacy policies. In addition, your firm may be required to give *consumers* a limited type of notice called a “short form initial notice.” In order to determine which notice requirements apply to your firm, you should answer the following questions:

- What NPI does your firm possess?
- Who are your customers?
- Who are your consumers?
- What are your current information sharing practices?<sup>13</sup>

The answers to these questions will help you determine which of the following types of notice is needed. The flowchart in Attachment A may also assist you in making this determination.

## **1. Notice to Consumers**

### **A. When Consumer NPI Is Not Disclosed (No Notice):**

You are not required to give any notice of your privacy policy to *consumers* as long as you do not disclose their NPI to any non-affiliated third party for any purpose other than those described in the exceptions listed in the “Opt Out Rights and Procedures” section below.<sup>14</sup>

### **B. When Consumer NPI Is Disclosed (Short Form Initial Notice):**

You may use an abbreviated notice to tell *consumers* that you may disclose their NPI to non-affiliated third parties. It cannot be used to provide notice to *customers*. The notice should be easily readable and describe how the consumer may request a copy of the firm’s privacy policy.<sup>15</sup>

## **2. Notice to Customers**

### **A. When Customer NPI Is Not Disclosed (Simplified Notice):**

You may provide a simplified notice to *customers* if you neither disclose nor reserve the right to disclose their NPI to any third party, including affiliates as well as non-affiliates. You may also use a simplified notice if you *do* disclose or reserve the right to disclose NPI to third parties, but only if the disclosure is permitted under the exceptions described in the “Opt Out Rights and Procedures” section below. The simplified notice should include: (1) the categories of NPI you do collect; (2) your policies and practices intended to protect the confidentiality, security, and integrity of NPI in your office (i.e., your “safeguarding” procedures); (3) your statement that you do not disclose and do not reserve the right to disclose NPI; and (4) your statement that you will make disclosures to non-affiliated third parties only as permitted by law.<sup>16</sup>

### **B. When Customer NPI Is Disclosed (Full Notice):**

You must provide a more comprehensive notice to *customers* if you disclose or reserve the right to disclose their NPI to any third party, including affiliates as well as non-affiliates, unless the disclosure is permitted under the exceptions described in the “Opt Out Rights and Procedures” section below. This notice must disclose your firm’s policies and practices about the following:

- What confidential information you may collect from or about a person;
- What confidential information you may disclose to other entities;
- The categories of non-affiliated third parties to which your firm may disclose confidential information;
- What your policy is on sharing information about former customers;

- What categories of confidential information your firm discloses under agreements with third party service providers (such as a broker-dealer or a sub-adviser);
- An explanation of a person's right to opt out of having confidential information disclosed to non-affiliated third parties, and what the person needs to do to opt out.
- Your office policies and practices intended to protect the confidentiality, security, and integrity of confidential information (i.e., your "safeguarding" procedures), including in general terms who is authorized to have access to this information.
- Notices required under the Fair Credit Reporting Act, if applicable.<sup>17</sup>

### **Opt Out Rights and Procedures**

With each short form or full notice, you must provide a reasonable way for a person to prevent your firm from disclosing NPI to non-affiliated third parties.<sup>18</sup> This process is called "opting out." Reasonable methods would include (1) a separate reply form, or a portion of the full notice that can be separated, with check-off boxes; (2) an electronic means to opt out such as through e-mail or through your firm's web site, if the person has agreed to receive your full notice electronically; or (3) a toll free telephone number that persons can use to call to opt out. It would not be considered reasonable to require a person to write their own letter to opt out.

### **Exceptions:**

There are no opt out rights for any disclosures of NPI you make to service providers or joint marketers, but you must disclose the nature of any information to be shared with a service provider or joint marketer and must enter into contractual arrangements to require the third party to maintain confidentiality of the information.<sup>19</sup> The opt out rights also do not apply to disclosure of confidential information in the following circumstances:

- When the consumer or customer has consented to, and has not revoked, the disclosure;
- For resolving consumer or customer disputes or inquiries;
- To persons holding a legal or beneficial interest relating to the consumer or customer;
- To persons acting in a fiduciary or representative capacity on behalf of the consumer or customer;
- To provide information to agencies assessing your firm's compliance with industry standards, and to your attorneys, accountants, and auditors;
- In connection with a proposed or actual sale or merger of your firm;
- To respond to a regulator's examination of your firm; or
- To comply with a civil, criminal, or regulatory investigation by federal, state, or local authorities.<sup>20</sup>

### **How, To Whom, and When to Send Notices?**

Reasonable methods of providing a notice include hand delivering a printed copy, mailing a printed copy to the last known mailing address, and for a person who conducts business with you electronically, posting the notice on the electronic site and requiring that the person acknowledge receipt of the notice prior to obtaining your service or product.<sup>21</sup> Simply posting a copy of your privacy notice in your office would not be considered a reasonable method of providing notice.<sup>22</sup> Also, simply telling someone on the telephone about your privacy policy would not be considered reasonable notice.<sup>23</sup>

You must provide the notice to a *customer* not later than the time you establish that on-going relationship, unless this would cause a delay in the customer obtaining your services **and** the customer agrees to accept the notice at a later date.<sup>24</sup> (For example, a new consumer gives you enough information over the telephone to establish a customer relationship and wants you to execute a transaction immediately.) For any person who is already your customer, you must provide the notice prior to disclosing any NPI, but no later than July 1, 2001.<sup>25</sup>

You must provide the notice to a *consumer* before you disclose any NPI about the consumer to any non-affiliated third party.<sup>26</sup> But, if the only non-affiliated third parties who would receive information from you are among those in the Exceptions discussed above, you are not required to provide any notice.<sup>27</sup>

### **Policy Changes and Annual Updates**

Any time you change your privacy policy concerning disclosure of any category of NPI, or any category of non-affiliated third party that would receive information from you, you must revise your notice. The revised notice and a new opt-out form or method must be given to each affected customer prior to any disclosure of information.<sup>28</sup>

Finally, you must annually provide (not just offer) your privacy notice to *customers*. You can define when the 12-consecutive-month year starts, but you must be consistent in applying it to all your customers. (For example, if you define a year as a calendar year, for a customer who opens an account on any day of year 1, you must provide the annual notice to that customer by December 31 of year 2.)<sup>29</sup>

You are not required to provide the notice to persons who no longer are your customers.<sup>30</sup> You are also not required to provide annual notices to persons who have previously requested that you not send them any information about the customer relationship, so long as your current privacy notice is available to that customer.<sup>31</sup>

## **Sample Clauses**

The following clauses are samples only. Please refer to the rules cited in the footnotes for further illustrations.<sup>32</sup> **WARNING:** You must be sure that any statement you make is accurate.

### **If you do not disclose information outside of the Exceptions:**

“We do not disclose any confidential personal information about our customers or former customers to anyone, except as permitted by law.”

### **To describe the categories of information you may disclose:**

“We may disclose the following kinds of confidential personal information about you:

- Information we receive from you on applications or other forms, such as [provide illustrative examples, such as “your name, address, assets, and income”]
- Information about your transactions with us, our affiliates, or others, such as [provide illustrative examples, such as “your account balance, investing history, and parties to transactions”]

### **To describe the categories of parties to whom you disclose information:**

“We may disclose confidential personal information about you to the following types of third parties:

- Financial service providers, such as [provide illustrative examples, such as “mortgage bankers, securities broker-dealers, and insurance agents”]
- Non-financial companies, such as [provide illustrative examples, such as “direct marketers, airlines, and publishers”]
- Others, such as [provide illustrative examples, such as “non-profit organizations”]

“We may also disclose confidential personal information about you to non-affiliated third parties as permitted by law.”

### **To describe disclosure to service providers or joint marketers:**

“We may disclose the following information to companies that perform marketing services on our behalf or to other financial institutions with which we have joint marketing agreements:

- Information we receive from you on applications or other forms, such as [provide illustrations, such as those described above]
- Information about your transactions with us, our affiliates, or others, such as [provide illustrations, such as those described above]

(NOTE: your customer must receive notice, but has no right to opt out of disclosure.)

**To explain the opt out right:**

“If you prefer that we not disclose confidential personal information about you to non-affiliated third parties, you may opt out of those disclosures; that is, you may direct us not to make those disclosures (other than disclosures permitted by law). If you wish to opt out of disclosures to non-affiliated third parties, you may [*describe a reasonable means of opting out, such as “call the following toll free number: (insert number)”*]

**To describe your policies and practices concerning protecting confidentiality:**

“We restrict access to confidential personal information about you to [*provide an appropriate description, such as “those employees who need to know that information to provide products or services to you.”*] We maintain physical, electronic, and procedural safeguards to comply with federal standards to guard your confidential personal information.”

### **SEC vs. FTC Rules**

While the Securities and Exchange Commission (“SEC”) has privacy jurisdiction over large investment adviser firms, the Federal Trade Commission (“FTC”) has privacy jurisdiction over investment advisers not registered with the SEC. The FTC has acknowledged that an investment adviser’s compliance with the sample clauses in the SEC rules will equate to compliance with the FTC rules.<sup>33</sup> Rules cited herein by footnotes are to both SEC and FTC regulations.

You may learn more about the rules and requirements by visiting these agencies online. For the SEC rules, go to [www.sec.gov/rules/final/34-42974.htm](http://www.sec.gov/rules/final/34-42974.htm). For the FTC rules, go to [www.ftc.gov/os/2000/05/65fr33645.pdf](http://www.ftc.gov/os/2000/05/65fr33645.pdf).

---

<sup>1</sup> Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (hereinafter GLBA).

<sup>2</sup> Section 504 of GLBA grants authority to the federal Securities and Exchange Commission to adopt privacy regulations for federal covered advisers. Authority is granted to the Federal Trade Commission to adopt privacy regulations for state registered investment advisers and certain other financial institutions. The SEC regulations governing federal covered advisers are found at 17 C.F.R. § 248, and the FTC regulations governing state registered advisers are found at 16 C.F.R. § 313.

<sup>3</sup> 17 C.F.R. § 248.18 and 16 C.F.R. § 313.18.

<sup>4</sup> 17 C.F.R. §§ 248.4 & 248.10(a), and 16 C.F.R. §§ 313.4 & 313.10(a).

<sup>5</sup> GLBA § 509(11), 17 C.F.R. §§ 248.3(j) & (k), and 16 C.F.R. §§ 313.3(h) & (i).

<sup>6</sup> GLBA § 509(9), 17 C.F.R. § 248.3(g), and 16 C.F.R. § 313.3(e). GLBA § 509(11), 17 C.F.R. §§ 248.3(j) & (k), and 16 C.F.R. §§ 313.3(h) & (i).

<sup>7</sup> GLBA § 509(4), 17 C.F.R. §§ 248.3(t) + (v), and 16 C.F.R. §§ 313.3(n) + (p).

<sup>8</sup> GLBA § 509(6), 17 C.F.R. § 248.3(a), and 16 C.F.R. § 313.3(a).

<sup>9</sup> GLBA § 509(5), 17 C.F.R. § 248.3(s), and 16 C.F.R. § 313.3(m).

<sup>10</sup> GLBA § 502(b), 17 C.F.R. § 248.10(a)(2), and 16 C.F.R. § 313.10(a)(2).

<sup>11</sup> 17 C.F.R. §§ 248.14(a), 248.13(b) & (c), and 16 C.F.R. § 313.14(a), 313.13(b) & (c).

<sup>12</sup> 17 C.F.R. §§ 248.12(b)(1) and 248.13(a)(2); 16 C.F.R. § 313.12(b)(1) and § 313.13(a)(2).

<sup>13</sup> GLBA § 503 describes the notice requirements, which are more fully set forth by regulation in 17 C.F.R. §§ 248.4 et seq. and 16

- 
- C.F.R. §§ 313.4 et seq.
- <sup>14</sup> 17 C.F.R. § 248.4(b) and 16 C.F.R. § 313.4(b).
- <sup>15</sup> 17 C.F.R. § 248.6(d) and 16 C.F.R. § 313.6(d).
- <sup>16</sup> 17 C.F.R. § 248.6(c)(5) and 16 C.F.R. § 313.6(c)(5).
- <sup>17</sup> GLBA § 502(e), 17 C.F.R. §§ 248.4 & 248.6, and 16 C.F.R. §§ 313.4 & 313.6.
- <sup>18</sup> 17 C.F.R. § 248.7 and 16 C.F.R. § 313.7.
- <sup>19</sup> GLBA § 502(b)(2), 17 C.F.R. §§ 248.13 - 248.15, and 16 C.F.R. §§ 313.13 - 313.15.
- <sup>20</sup> 17 C.F.R. § 248.15 and 16 C.F.R. § 313.15.
- <sup>21</sup> 17 C.F.R. § 248.9(b)(1) and 16 C.F.R. § 313.9(b)(1).
- <sup>22</sup> 17 C.F.R. § 248.9(b)(2) and 16 C.F.R. § 313.9(b)(2).
- <sup>23</sup> 17 C.F.R. § 248.9(d) and 16 C.F.R. § 313.9(d).
- <sup>24</sup> 17 C.F.R. § 248.4(e) and 16 C.F.R. § 313.4(e).
- <sup>25</sup> 17 C.F.R. § 248.18(b) and 16 C.F.R. § 313.18(b).
- <sup>26</sup> 17 C.F.R. § 248.4(a)(2) and 16 C.F.R. § 313.4(a)(2).
- <sup>27</sup> 17 C.F.R. § 248.4(b) and 16 C.F.R. § 313.4(b).
- <sup>28</sup> 17 C.F.R. § 248.8 and 16 C.F.R. § 313.8.
- <sup>29</sup> 17 C.F.R. § 248.5 and 16 C.F.R. § 313.5.
- <sup>30</sup> 17 C.F.R. § 248.5(b) and 16 C.F.R. § 313.5(b).
- <sup>31</sup> 17 C.F.R. § 248.9(c)(1)(ii) and 16 C.F.R. § 313.9(c)(2).
- <sup>32</sup> SEC sample clauses are found in an appendix to 17 C.F.R. § 248. FTC sample clauses are found in an appendix to 16 C.F.R. § 313.
- <sup>33</sup> At 65 Fed. Reg. 33649, in its explanation of the new privacy rules, the FTC stated: "The Commission understands that the NCUA and SEC have issued, or will issue, final rules with examples that are tailored to entities under their jurisdiction..... (C)ompliance by interstate (sic) securities broker-dealers and investment advisers that are not registered with the SEC with applicable examples in the SEC rule will constitute compliance with the Commission's rule."